Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Основы защиты информации

Практическое задание №14

«Изучение стандартных средств для реализации приложений, использующих симметричное и ассиметричное шифрование с использованием библиотеки System.Security.Cryptography»

Подготовила: студентка ФИТ 2 курса 5 группы Буранко В.Д.

Проверил: асс. Берников В.О.

Цель: Изучить модель криптографии .NET Framework, Основные классы и структуры данных, разработать приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования.

1. Какие симметричные алгоритмы шифрования Вы знаете?

Простая перестановка, одиночная перестановка по ключу, двойная перестановка по ключу, перестановка «Магический квадрат Дюрера», шифрование Цезаря, система Тритемиуса, шифрование Трисемуса, система Плейфера, система Вижинера, шифр «Двойной квадрат» Уитстона.

1. Какие ассиметричные алгоритмы шифрования Вы знаете?

RSA, алгоритм Диффи-Хеллмана, алгоритм Эль-Гамаля.

1. Основное назначение библиотеки System.Security.Cryptography?

Пространство имен System.Security.Cryptography содержит поддержку наиболее распространенных симметричных, асимметричных и хешированных алгоритмов криптографии. Он также включает полезный класс для шифрования и расшифровки потоков. Т.е. эта библиотека предназначена для любых задач по защите данных.

1. Влияет ли размер ключа на криптостойкость алгоритма?

Да, т.к. при увеличении размера ключа становится значительно сложнее его вычислить или подобрать, пусть и оригинальные вычисления также становятся дольше.

1. Назовите основные классы библиотеки System.Security.Cryptography?

Библиотека System.Security.Cryptography содержит более 100 классов, и этот список постепенно расширяется вследствие разработки новых алгоритмов шифрования. К основным классам обычно относят:

SymmetricAlgorithm – абстрактный класс для всех симметричных алгоритмов;

AsymetricAlgorithm – абстрактный класс для всех ассиметричных алгоритмов;

DES – абстрактный класс для различных реализаций DES алгоритмов;

RSA – абстракция шифрования с открытым ключом RSA;

DSA – абстракция шифрования с открытым ключом DSA.

Вывод. Изучила модель криптографии .NET Framework, основные классы и структуры данных, разработал приложение для шифрования файлов использующих симметричные и ассиметричные алгоритмы шифрования.